"Process and system of secure access to a data processing server"

The hereafter disclosed invention regards a process allowing to increase the level of security of the authentication protocol related to a request for accessing a data processing server. The invention further concerns a system of secured access using this process.

A person who requests access, or "client", commonly uses a personal computer or a workstation equipped with means of connecting to a communication network such as Internet.

A server is a computer equipped with means of connecting to the same network. Its aim is to get the client in relation with various services such as data bases.

A conventional procedure of a client's access takes place in three phases:

- accessing the server site by setting up a connection (e.g. TCP/IP) through a public or proprietary data communication network (e.g. Internet),
- entering a "user identification", and then
- entering a client's password.

Access is denied if the identification/password couple does not match the information stored in a "identification" named data base which is managed either by the server itself or some dedicated intermediate server.

Known procedures exhibit numerous weaknesses facing such attacks as theft of the identification/password couples using an automated password search software or some connivance on the "server" side allowing to know the authentication data base contents.

Various solutions or reinforcing the access security are known:

- on the server side, an auxiliary feature for generating random and/or encrypted passwords, but necessitating the client owns a device synchronised with the server to generate a short life, pseudo random password depending on the date/time;
- personal computer equipped with an electronic card ("smart card") reader which secures the access according to a protocol analogous to those used with credit cards; thus the client's terminal used for connecting to the network needs a special peripheral;
- identification of the user's computer using an identification code the microprocessor manufacturer has on-chip engraved; the access is thus secured using some component(s) of the server known by the server; however the drawback is that the client cannot perform an access outside a limited number of listed machines.

Moreover known encryption systems such as RSA involve high processing power to provide a convenient level of security.

From the WO9731306 document a process is known for providing authentication data to a user using SMS message transmission to a mobile telephone through a mobile telephony network.

The US5668876 document discloses a process of authenticating a user of an electronic service provider connected to a first communication network, such user owning a mobile telephone. This authentication process comprises:

- a step of transmitting a request code over a second communication network such as a mobile telephony network,

- this code being received on a requesting user personal unit,
- a step of generating within the personal unit an output code, this output code being then either transmitted from the personal unit to the authentication centre, or entered on a user terminal linked to the first communication network,
- the step of comparing within the authentication centre the answered code and the expected code, and
- a step of granting access to the electronic service in case the comparison is satisfactory.

The above cited securing processes exhibits the drawback of needing the active cooperation of a mobile telephony operator and sometimes an adaptation of the mobile telephony equipment involved in those processes.

The hereby disclosed invention object is to propose another solution which does not necessitate the active cooperation of a mobile telephony operator and which would be as well highly reliable, flexible and low-cost.

The invention proposes a process of securing the access to a data processing server from a client site through at least one first communication network, the server comprising means for handling a user of the client site authentication protocol, comprising a sequence of receiving and processing the client site user authentication data, and a sequence of transmitting from the server site to a communication equipment

owned by the client site user through a second communication network.

According to the invention, this transmitted message is a vocal message aimed to be directly processed by said user for generating an authentication password provided for being transmitted to said server site through one or the other of said first and second communication networks.

The idea at the base of the present invention is thus to implement in the authentication protocole a mobile phone with its function of vocal transmission and not with its function of transmitting digital information or short messages, the server site being provided with means permitting it to call the mobile phone and to transmit to it a vocal message.

The first communication network can be the Internet network and more generally any communication network wired or unwired, for example a mobile communication network.

The second communication network implemented in the securing process acordiing to the invention is preferably a mobile communication network, but could ne a fixed communication network able to communicate with mobile communication equipments.

The process according to the invention does not require on the side of the client site any special identification computer device, either integrated or peripheral. It requires the possession of a conventional mobile phone, an apparatus that tends to be generalized among professionals and public. The equipment cost on the side of the server is also low since a standard modem of the type including a vocal synthesis unit can for example be used for achieving the connection with the mobile phone network.

Another advantage according to the invention lie in the fact that neither the server nor the client station need high processing power

when compared to encryption systems, hence substantially reducing the cost of a system according to the invention. A reduction of the implementation cost and furthermore no additional cost when procedures change vs. security solutions based on hardware may be foreseen as well.

One will notice that the security carried by the invention is further enhanced by the procedure of identification by the network which registers the mobile telephone in itself. In the case of the GSM standard this procedure implements a specific electronic component (the SIM card) plugged into the set, and the ability of the user to own a changeable password (the PIN code) which must be entered when the telephone is switched on.

In of theft of the mobile telephone or of the SIM component, the latter may be instantly discarded by all the GSM networks after a simple call to the mobile phone registering network provider. One can foresee that access to the network will be denied after a theft statement.

The process according to the invention allows to reuse existing procedures though adding a level of security. It may apply as an add-on of any access software.

In such case the authentication data requested from the user may be the [client identification code / password] (ID/PWD) of the authentication protocol known in the prior technical art, so that the direct or indirect knowledge of this couple will not be enough any more to be granted access to the server.

In a first embodiment, the process according to the invention comprises the steps of:

- requesting authentication data from the client site through the first communication network;

- process this data and searching an authentication data base for the call number of the mobile communication equipment owned by the client site user;
- after setting up the communication with the aforesaid mobile communication equipment, generate a random or pseudo random password;
- transmit through the second communication network a voice message comprising the aforesaid random password;
- request from the user, through the first communication network, an authentication password derived from the aforesaid random or pseudo random password; and
- authenticate the aforesaid authentication password.

As an example, the authentication password may match the server generated random or pseudo random password and transmitted through the mobile communication equipment.

However the authentication password may be so designed to result from an operation based on a key known by the client user and included within the server authentication data base, the authentication step comprising a step of converting the aforesaid authentication password into a random or pseudo-random password using the aforesaid key.

As an example the key may be a known personal constant to be added or subtracted for yielding the server password. It may as well be a logical operation such as a transposition.

The identification data requested from the client may be an [identification / password] couple.

Preferably, the step of requesting the authentication password from the client takes place within a predetermined duration beyond which the authentication is denied.

In another embodiment of the invention based process, this process comprises those steps performed on the server side:

- requesting identification data from the client site through the first communication network;
- process this data and search an authentication data base for the call number of a mobile communication equipment owned by the client site user;
- calling the aforesaid mobile communication equipment through at least one second communication network;
- in case the communication with the aforesaid mobile communication equipment is set up, transmit a voice message which requests from the user to send an encryption key;
- receiving and recognising the encryption key transmitted by the client by means of the mobile communication equipment keyboard;
- deciphering, according to the aforesaid encryption key, an authentication password transmitted by the client through the first communication network, this authentication password resulting from an encryption of a client password performed at the client site using the encryption key; and
- authenticate the client password which results from deciphering the authentication password.

Another possible design consists in uploading though the second communication network access data resulting from the voice message transmitted by the server through this second network and implement this in several ways. As an example the following process may be foreseen:

A voice message is received through the second communication network by a client user on his mobile telephone, in response to a request sent to the server through a first communication network from a terminal connected to this network. As an example this voice message indicates a piece of data to be processed on the terminal.

The client user then performs a predetermined operation (e.g. a translation or any simple or complex change) upon the indicated piece of information and then types the result onto his mobile telephone keyboard.

This specific embodiment of the invention is specially adapted to such terminals as electronic payment terminals equipped with raw data entry means.

According to another aspect of the invention, a system of securing the access to a data processing server from a client site through a first communication network is proposed, implementing the invention process, this system comprising means at the server site to handle a client site user authentication, means for receiving and processing the client user identification data, and means for generating and transmitting from the server site through a second communication network a message to a user owned communication equipment, characterised in that the system is organised for transmitting over the second communication network a voice message intended to be processed directly by the aforesaid user for generating an authentication password intended to be transmitted to the aforesaid server site through the aforesaid first communication network.

This system may further advantageously comprise, in a first implementation embodiment:

- means for searching a call number of a user owned mobile communication equipment, in response to identification data received from a client site to request an access;
- means for calling the aforesaid mobile communication equipment through at least one second communication network;
- means for generating a random or pseudo random password;
- means for authenticating an authentication password received from the client site through the first communication network, characterised in that it further comprises:
- means for sending a voice message containing the aforesaid random password upon the second communication network,
- means for requesting the user of the aforesaid client site to supply, though the first communication network, an authentication password derived from the aforesaid random or pseudo random password.

In a second embodiment of the invention, the system according to the invention may advantageously further comprise:

- means for requesting to the client site identification data through the first communication network;
- means for processing said data and searching in a authentication data base a number for calling a mobile communication equipment detained by the user of the client site;
- means for calling the aforesaid mobile communication equipment through at least a second communication network,
- means for emitting a vocal message requiring the transmission of an encryption key by the user;
- means for receiving and recognizing the encryption key transmitted by the client via keys of the mobile communication equipment;

- means for deciphering by means of said encryption key an authentication password transmitted by the client through the first communication network, the aforesaid identification password resulting from the encryption of a client password performed on the client site using the encryption key, and
- means for authenticating the client password resulting from deciphering the authentication password.

The process based on the invention can also be reinforced by foreseeing to automatically disable the access to the server as soon a predetermined number of attempts have failed at any stage of the entry steps, and considering to request the mobile telephony provider to instantly disable the telephone set.

According to another feature of the invention, it is proposed to implement the securing process of the invention within a system of authenticating digital creations, comprising third party services of date/time stamping, authenticating and archiving all connected to a first communication network, characterised in that each third party site embody software means for (i) sending securing data in voice mode through a mobile communication equipment dedicated to the client site and connected to a second communication network, and (ii) for receiving from the aforesaid client site an authentication password resulting from the aforesaid authentication data.

The present invention will be better understood and further advantages will be highlighted by the following description of two examples of implementation of the system and related processes according to the invention, this description being made in reference to the attached drawings:

- Figure 1 is a synoptic diagram of the first example of implementation of the system according to the invention;
- Figure 2 is a flowchart of the authentication process performed by the server which operates the Figure 1 system;
- Figure 3 shows in diagrammatic form a screen page generated by the server and used by the client for the Figure 2 authentication process transaction;
- Figure 4 is a synoptic diagram of the second example of implementation of the system according to the invention;
- Figure 5 is a flowchart of the authentication process performed by the server which operates the Figure 4 system;
- Figure 6 shows in diagrammatic form a screen page generated by the server and used by the client for the Figure 5 authentication process transaction; and
- Figure 7 is a synoptic diagram to illustrate an application of the invention for copyrighting digital creations.

As shown diagrammatically on the Figure 1, a first example of implementation of the invention comprises:

- on a client site 1, a personal computer 2 equipped with a modem 3 for accessing a data communication network 4, and a personal mobile telephone set 5 registered by a mobile telephony network 6, e.g. using the GSM standard; and

- on a server site 7 a computer based server 8 which runs a software designed for handling the client process of accessing the services 9 according to the invention, noticeably the client authentication protocol; the computer equipment comprises: a modem 10 which enables the computer to gain access to the telephony communication network 6 and to perform a telephone number dial, means for generating a "MPA" random or pseudo random password, and a speech synthesis circuit 12 allowing to

send to the mobile telephone 5 a message comprising the random generated MPA password necessitated by the authentication protocol. The computer 8 is linked with a "BDA" authentication data base holding for each client a triplet ["ID" identification code/"MPC" client password/matching personal mobile telephone number].

The secure access process is performed as follows.

The user located at the client site 1 asks access to the server. The connection between the client site 1 and the server site 4 through the data communication network 4 is established in a known conventional fashion by means of the modem 3 of the client site, the switched telephony network, and a general purpose Internet network access provider.

The server returns a page 15 that is displayed on the personal computer screen; this page is shown in Figure 3, and comprises three entry fields: the first two fields are for the conventional couple [ID identification code/MPC client password]. The third field 18 is for a "MPAUT" authentication password which shall be derived from the "MPA" random or pseudo random password which will be sent to the client site 1 by means of the mobile telephone 5. This MPAUT authentication password here matches the MPA random or pseudo random generated by the server.

As a first step, the client enters his [identification code/password], ID/MPC couple, which is already secured by any known method based on the BDA authentication data base.

Referring to the Figure 2 flowchart, the next invention specific steps of the protocol will only be performed by the server if the identification/password checking step 20

is granted, as a prerequisite.

If so, the next step 21 consists in dialling by means of the modem 10 the mobile telephone number retrieved in the BDA authentication data base. At the next step 22, if the telephone communication is established with the mobile telephone (e.g. "hook-up" signalled by the server site modem 10), the server generates a MPA random password and sends it to the mobile telephone 5 by means of its speech synthesis circuit. The next step 23 consists in waiting for the authentication password MPAUT entry by the client at the client site within a predetermined time-out delay 24. If at step 25 the entered MPAUT password is compliant, the authentication is granted and then the client is entitled to access the services 9 of the server.

Thus, an authentication failure takes place under the following circumstances:

- conventional ID/MPC couple authentication is denied,
- the telephone call fails to establish the communication,
- wrong or missing MPAUT within the predetermined time-out delay.

Other implementation embodiments are possible, specially regarding the server password derivation from the random MPA password, which can result from combining the random MPA password with a personal client's arithmetic or logical key recorded in an additional field by the BDA data base together with the ID identification code, the MPC client password and the mobile telephone number fields. The server will be provided means for processing the generated MPA password in order to proceed to the authentication step.

Figures 4 to 6 relate another implementation embodiment of the system according to the invention, differentiated by having the client site 1 further equipped with encryption means 30 suited to encrypt the MPC password after the client has entered it and before it is sent through the data communication network 4 to the server site 7. On the server site side, this embodiment is differentiated by means 31 of recognition of a signal sent by the client by typing on his personal mobile telephone set 5 keyboard and means 32 to decipher the MPC client password according to an encryption key which is transmitted by the client by typing on his mobile telephone keyboard. The BDA authentication data base only holds two fields in such case, one holds the ID code and the other holds the MPC client password. The after deciphering authentication protocol matches the protocol known in prior art.

The secured access process using this system is performed as follows.

In response to an access request by the client using the client site 1, the server displays on the personal computer 2 a screen page shown at Figure 6, which compared with the first embodiment comprises only two entry fields 36 and 37 matching the conventional couple [ID identification code/MPC client password]. Just after the MPC client password entry, means 30 encrypt the client entered password according to an encryption key which is solely known by the client. This encrypted client password corresponds to the password named "authentication password" in the process according to the invention.

Referring to the Fig. 5 flowchart, the authentication protocol steps take place as follows.

Firstly, at step 40 , the server which has received the encrypted password together with the ID code, identifies the client from the ID identification code and then at step 41 searches the BDA authentication data base

for the mobile telephone number. The next step 42 is of dialling the mobile telephone number. If at the next step 43 the communication is established with the mobile telephone, the serve send by means of its voice synthesis means 12 a message (step 45) to point out that it is expecting the user to enter the encryption key by means of the mobile telephone keyboard. The step 46 is of waiting for this key entry within a predetermined time-out delay. The next step 47 is of authenticating the MPAUT received through the network 4 by deciphering this password using the key and then authenticating the resulting client password according to the authentication protocol. If the MPC client password complies (step 48) the authentication is granted and the client may then access the server provided services 9.

Thus, an authentication failure takes place under the following circumstances:

- the telephone call fails to establish the communication,
- wrong or missing entry of the MPC client password and the encryption key.

The securing process of the invention may find an especially interesting application when it is implemented in a system of digital creations authentication and copyright as shown diagrammatically in Fig. 7. This system, implemented based on the Internet and the Web, comprises a first site S1 that provides a time stamp third party function, a second site S2 that provides an authentication third party function, and a third site S3 that provides an archiving third party function. The system may as well provide - though not necessarily - an authentication services provider site SP offering a portal and switching function to the aforesaid sites.

Each of those third parties is equipped with a software implementing the securing process of the invention. When an client - author or owner of some digital creation – addresses each of the S1, S2 and S3 third party sites, either directly or indirectly through the portal service provider SP, the securing process of the invention is performed, providing to the client MPA1, MPA2 and MPA3 passwords and then the client sends through the Internet MPAUT1, MPAUT2 and MPAUT3 passwords each dedicated to the addressed third party site. Obviously, if needed the legal authority direct access to the information and data stored at each site may be granted in the interest of the clients which use the authentication system of the invention.

Obviously, the invention is not bounded within the aforesaid examples and many variations of those examples may be provided without leaving the invention framework. As a special case, the securing process of the invention may also concern Internet access mobile equipment using the WAP (Wired Access Protocol) technology. One may foresee that a same mobile equipment will provide together an access to a first WAP communication network and to another mobile communication network to be used as a vector of transmitting the passwords from a site which implements the securing process of the invention.